Protecting Data, Protecting Residents

10 Principles for Responsible Municipal Data Management

The need for guidance in municipal data practices around the United States of America is now acute, given the shift in the national political environment. In pursuit of fulfilling his campaign promise of deporting millions of people from the nation, President Trump promulgated Executive Order: Enhancing Public Safety in the Interior of the United States on January 25, 2017.

This order aims to achieve mass deportation goals by upending the existing relationship between US Immigrations and Customs Enforcement (ICE) and local governments, moving DHS away from their existing Priority Enforcement Policy -- which focused deportation efforts on people convicted of crimes -- and by re-establishing the Secure Communities program, which makes all people without valid immigration documentation a target for immediate deportation. The executive order further attempts to enforce this policy by conditioning federal funding on local governments' cooperation with the broadened deportation regime.

This executive order places local governments in a difficult situation. Under the new policy, immigrants in cities are likely to feel that all contacts with the government pose a danger to them or to family members. For cities with significant immigrant communities, this has the potential to destroy the normal fabric of municipal life: preventing children from going to school and adults from going to work, preventing people from getting help when they need it, and heightening tensions between local police and the communities they serve. The situation is not improved by the continuing legal uncertainty. Given judicial precedent, there remains a reasonable chance that legal review will limit aspects of the executive order. Between the disruption to city services and the potential unconstitutionality of the order, all cities should consider reviewing a range of responses to the order at present.

Local governments are asked to support federal deportation policy in two ways: through the temporary detention of immigrants on ICE request and through sharing locally-collected information about undocumented immigrants. Most local law which addresses the obligations of local government towards federal immigration mechanisms – e.g., the use of the National Crime Information Center (NCIC) database for all contacts or local compliance with ICE "detainer" requests – specifically addresses the responsibilities of law enforcement.

However, while law enforcement is the primary local department implicated in federal immigration action, it is not the only one. Any local agency or department which disburses federal grants is likely to share data back to the federal government as part of its work. Moreover, while law enforcement agencies have received advice from a number of sources over the last decades' changes in immigration regime, other local departments have received fewer recommendations for action. This resource address these non-law enforcement departments that understand the high stakes for the residents whose data they hold and want to be

deliberate in the ways that they choose to share immigration-relevant information with the federal government.

All local government departments have a responsibility to revise their data management protocols so they do not inadvertently undermine official municipal policy. While municipal data may not be collected, kept or shared with the intention of endangering residents newly vulnerable on the basis of their documentation, religious, or national status, it may nonetheless come to be used that way.

Municipal departments need to consider their formal data collection, retention, storage and sharing practices, their informal data practices, as well as their vulnerability to unsanctioned data theft in order to protect the civil and privacy rights of their residents most effectively.

The following guidelines aim to strengthen local data management practices under these circumstances.

Limit Collection

1. Do not collect sensitive information (e.g., related to documentation status, national or religious identity) unless it is absolutely necessary to do so.

To best protect residents' data privacy, departments should focus primarily on appropriately limiting the initial collection of data which would make residents vulnerable if it were shared. Restricting the collection of this kind of information has long been considered best practice for privacy protection. This general recommendation, however, takes on new urgency given the increase in political relevance of residents' personally identifiable data. Since databases may end up being subpoenaed or stolen, merely securing this data should not be seen as a sufficient solution.

To limit the unnecessary collection of sensitive information, departments must first learn all of the ways that they currently collect it. Each department should review all forms, applications and pamphlets so it can be aware of and evaluate the necessity of each question that is likely to produce this data, including:

- Questions about citizenship status
- Questions which may serve as a proxy or starting point for evaluating citizenship status, including:
    - requests for SSN or ITIN
    - requests which reveal non-English monolingual status
    - requests for nationality
- Questions about religious identity

Chicago provides an example of what a legal articulation of this principle looks like in Section 2-173-060 of its Municipal Code:

> All applications, questionnaires, and interview forms used in relation to City of Chicago benefits, opportunities, or services shall be promptly reviewed by the pertinent agencies and any questions regarding citizenship or immigration status, other than those required by statute, ordinance, federal regulation or court decision, shall be deleted within 60 days of the passage of this ordinance.

2. Where sensitive information is needed for decision-making, evaluate whether that information can be gathered without written documentation.

In the interest of limiting the production of sensitive data, departments which must ask questions that directly or by proxy reveal immigration status should determine whether it would be possible to do this verbally.

Employees could limit their collection of sensitive information and help build trust at the same time by letting residents know that they are protecting them through limiting the unnecessary collection of information. They would then verbally ask residents the relevant question (in person or over the phone) before beginning to document, and then simply take the action that the answer requires rather than recording the answer to the question itself.

For example, if a department needs to determine whether a potential applicant is eligible for a federally funded benefit and needs to know whether the applicant is a US citizen, the department staff could first ask this question verbally. Based on the answer, the potential applicant could then be advised either to apply for the federally-funded benefit or instead directed to a locally-funded program which does not require documentation of citizenship status. Applicants would receive the appropriate service, but no sensitive data would be created.

Improve Storage Practices

3. Regularly delete sensitive data where retention is not legally required.

Departments should be sure that all employees are following current record retention and disposal schedules. Departments should also evaluate all discretionary records retention schedules for data which contains personally identifiable information and seek to minimize, as much as possible, the official retention periods for that data.

4. Do not create or retain specialized, personally-identifiable databases of vulnerable groups of residents.

It is important not to create data unintentionally about vulnerable populations through the process of service delivery. While it may seem obvious not to create a database of people of a single citizenship status, sexual identity or religion, it is easy to create these databases accidentally when attempting to provide a service to the group in question. A list of people eligible for a particular service, or a list of people who have received a particular benefit, can effectively become a documentation of their status if their status is not rendered non-identifiable.

The best policy for ensuring that data cannot be used for actions a municipality does not itself support is to prevent the creation of it. If data must be retained, however, there are several different approaches for mitigating the problem of maintaining a list of vulnerable residents.

- *Anonymization*: Existing guidance for cities that want to secure data created through municipal ID programs describes how cities can solve the problem of identifiable service recipients through hashing all of the maintained identifiable data. This is a technical approach where information is transformed with an algorithm to produce a string of characters that can't be changed back into its original form, although identical information hashed in the same way will always come out the same way (and so can be used to confirm identity.)

- *Diversity:* Ensuring that, on any one sensitive variable, the database contains sufficient diversity to effectively hide the sensitive population makes the database less dangerous. If, for example, local libraries added patron pictures and addresses to all patrons' cards, library cards could serve as de facto municipal IDs. However, since the sensitive population makes up only a very small subset of all library card holders, the database is less useful as a way to identify them. This approach does become less useful if the dataset can be combined with other data in a way that reveals the sensitive population residing within the total.

- *Proactive destruction policies*: Maintaining a clear rationale for the destruction of the dataset may also be an acceptable approach, if it is sufficiently defined. However, New York City's recent experience of being prevented through legal action from deleting the data it collected about its vulnerable municipal ID holders demonstrates the inherent danger of this approach.

- *Legitimating non-government alternatives*: For some services that would require the collection of sensitive data, governments can choose to express support for security-minded non-governmental alternatives rather than providing the service themselves. The cities of Cincinnati and Greensboro, for example, both directed local officials to accept identification cards issued by local non-governmental organizations as an acceptable, limited form of resident identification.

5. Where sensitive information is collected, do not store it with less-protective third parties.

Once data has moved from its original location to a third party, US law offers it less protection. As a result, where departments collect data which reveals citizenship or other vulnerable status, they should avoid hosting or sharing it with a third party vendor. If departments must share data with a vendor, they should be aware that the federal government may ask the vendor directly for the information they hold and proactively attempt to limit that sharing through clear language in their contract. For better security, the department might consider contracting with a company based outside of the US to limit the effectiveness of national security letters. (Even a domestic company which stores information overseas might offer some degree of protection, per the Microsoft Ireland case.)

6. Encrypt sensitive data and communications to limit the potential for data theft.

Just as departments need to be cautious about storing data with third-party vendors, so too they need to be conscious of the dangers posed by data that is insufficiently secured on their own systems. Data encryption practices that governments can implement to improve the security of all of their data include:

- Deploying HTTPS across all municipal web services. The federal government has provided useful resources to explain the importance of HTTPS and provide models for migration to HTTPS that other governments could adopt.
- Requiring full hard disk encryption on servers and also on other devices, so that there won't be a breach if devices are lost.
- Where feasible, select end-to-end encrypted methods of communication over those that are not end-to-end-encrypted. Care should be taken, however, that government communications through encrypted channels still follow applicable public records laws.

Improve Oversight of Data-Sharing

7. Inventory all policies and practices which result in the sharing of information on individuals' citizenship or other sensitive status.

It is unlikely that any government has a comprehensive picture of the ways that it shares its data with other governments and the public. In order to create that picture, to ensure that the public is aware of existing data-sharing requirements, and to know how to develop further policy, every department should develop a complete inventory of the ways that it formally (via law or regulation) and informally (via phone or emailed request) provides access to the data that it collects and maintains. Once this inventory is created, a department head should review the

inventory, evaluating the relationship between existing practice and data-sharing policies that the city has already or wishes to promulgate.

8. Publicly document all policies, practices and requests which result in the sharing of information about individuals' citizenship or other sensitive status.

The provision of "notice and consent" opportunities is key to compliance with the Fair Information Practice Principles, a common framework for evaluating the protection of individuals' data privacy. In line with that obligation, it's important to ensure that governments are letting their residents know what aspects of their data are being shared and with whom.

After departments have inventoried their data-sharing policies and practices, they should make those inventories publicly available so that the public can be aware of the data streams that are shared with the federal government and other requesters. Once departments are generally aware of the particular datasets that must be shared, it would be appropriate for them to inform residents of this at the point of data collection so that residents can make their own choice about participating, if they have the option.

Unless there is a clear legal reason why the residents cannot be informed of the request, any specific request for particular individuals' citizenship (or other sensitive) status should also be relayed to the affected residents. Governments who can commit to doing this should also publicize this policy to increase public confidence that governments will avoid sharing individuals' sensitive data without their knowledge.

9. Create policies which limit individual employees' discretion on data-sharing.

If it is determined that a government wants to limit data-sharing about sensitive issues to situations where there is a clearly legal requirement for that sharing, it can create policies to do so. For example, a restriction on informal sharing information about an individual's immigration status, without specific legal cause to do so, might look like this provision in the 2017 Oak Park "Welcoming Village" Ordinance:

> No agent or agency shall request information about or otherwise investigate or assist in the investigation of the citizenship or immigration status of any person unless such inquiry or investigation is required by an order of a court of competent jurisdiction. Notwithstanding this provision, the Village Attorney or the Village Attorney's designee may investigate and inquire about immigration status when relevant to potential or actual litigation or an administrative proceeding in which the Village is or may be a party.

Another approach to limiting the range of data-sharing practice may be to create a policy which requires City Council oversight of new arrangements to share data that includes sensitive data like citizenship status, in line with the ACLU's recommended provisions for ensuring City Council oversight of any new surveillance technology or data-sharing initiative.

10. Create a municipal oversight body to ensure that the city's protocols for data protection are adequate, well-observed, and legal.

To further build the government's capacity to oversee and protect resident data, cities should consider creating an internal data security oversight body to keep government IT, legal departments, and program heads in good communication on this topic. This body would constitute a formal point of decision-making for questions about the legality or desirability of departments' data management practices. A body which brings together technology and legal expertise is in the best position to evaluate both the legal and the practical viability of any policy or procurement option.

The ordinance establishing Oakland's Privacy Commission provides one model for articulating the variety of necessary expertise:

> All members of the Privacy Commission shall be persons who have an interest in privacy rights as demonstrated by work experience, civic participation, and/or political advocacy. No member may be an elected official. Members of the Privacy Commission may represent the following criteria, with no more than two (2) members representing any one criteria and at least one from each criteria to the extent possible:
>
> 1. an attorney, legal scholar, or activist with expertise in privacy, civil rights, or a representative of an organization with expertise in the same
> 2. a past or present member of member of law enforcement who has worked with surveillance equipment and other technology that collects or stores citizen data;
> 3. an auditor or certified public accountant;
> 4. a hardware, software, or encryption security professional;
> 5. a member of an organization which focuses on government transparency and openness or an individual, such as a former government employee, with experience working on government transparency and openness.

A data security oversight body could also be charged with testing the current practices in different ways. For example, the body could contract with an external company that would test the government for the robustness of its security measures. The body could also contract with external security analysts to determine the impact of the "mosaic effect" on the government's current public or shared data with regard to rendering vulnerable populations identifiable.

Conclusion

This paper represents a first step towards communicating the kinds of policies and practices that will help local governments manage their data in a way that allows them to fulfill their public

commitments. We look forward to the development of further work in this area, as the new administration matures in its approach to intergovernmental relations.

For local governments, the upcoming period also represents a time of learning and figuring out what works best. Nonetheless, it is obvious that data management practices will need to be a part of this process. Where cities seek to express to all residents that they will continue to protect them, they will need both to positively communicate this intention to their residents and also to ensure that they are, in fact, effectively protecting their residents' information. Following these principles will help city departments and agencies know they are doing all they can to keep both residents, and their data, safe.